Reconnaissance faciale, le temps de la redevabilité ? Quelques réflexions sur le rapport d'information " sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles "

Caroline Lequesne

Reconnaissance faciale, le temps de la redevabilité ? Quelques réflexions sur le rapport d'information « *sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles* ».

Caroline LEQUESNE ROTH
Maître de conférences HDR en droit public, Université Cote d'Azur

Ceci est la version longue (et antérieure) d'un entretien paru au *Recueil Dalloz*, D. 2022. 1256.

Quels sont le contexte et les enjeux du rapport ?

Alors que le printemps 2021 amorça la juridicisation des enjeux éthiques de l'intelligence artificielle (IA), le printemps 2022 laissa place aux débats quant à la nature politique de ce droit émergent. Le *momentum* est décisif : les choix de gouvernance, d'architecture et de régime dessineront l'économie de nos rapports aux technologies du XXIe siècle et avec elle, notre modèle civilisationnel. La question des technologies de surveillance occupe, au sein de ces débats, une place centrale. Cette dernière se comprend au regard de la mise en tension exacerbée des droits fondamentaux qu'elle opère : peut-on admettre, et dans quelles limites, que la technologie renforce l'arsenal sécuritaire sans renoncer au droit à la vie privée, à celui se mouvoir librement, à la liberté de manifester ou d'exprimer librement ses opinions dans l'espace public ? Si l'Union européenne esquisse les premiers éléments de réponse en matière de reconnaissance faciale, sa proposition de règlement sur l'IA laisse aux États une large marge d'interprétation. C'est dans ce contexte que la commission des lois du Sénat a engagé une mission transpartisane, qui a livré ses conclusions dans un rapport d'information « *sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles* » en mai dernier. En l'absence de dispositions nationales idoines, les sénateurs ne cachent pas une double volonté, soutenue par la contingence : celle de mobiliser pleinement les technologies de surveillance pour la sécurisation des événements sportifs à venir, d'une part; celle d'assurer la « souveraineté technologique » des entreprises françaises et européennes dans la course à l'innovation de l'autre : « *[i]l n'est pas acceptable que l'encadrement de la recherche et développement au niveau français et européen obère l'élaboration de solutions techniques souveraines* ».

Quelle approche préconise la mission ?

Pour ce faire, la mission défend une approche expérimentale. Le rapport écarte l'élaboration d'un régime général à la faveur d'une démarche incrémentale sur trois ans, « *oblige[ant] le Gouvernement et le Parlement à réévaluer le besoin et recadrer le cas échéant le*

dispositif en fonction des résultats obtenus ». Ce choix, politique, se veut celui de la prudence bien qu'il présente des risques. Les travaux doctrinaux sur les « *sandbox* » ont mis en évidence, par le passé, l'insuffisante prise en compte des enjeux démocratiques qui a conduit à légitimer et institutionnaliser des usages sans cadre adapté, ni assentiment citoyen. L'expérimentation doit aussi, et avant tout, être celle d'un cadre idoine offrant de solides garanties en termes de transparence, de redevabilité et de démocratie. La mission s'en fait partiellement l'écho en proposant la mise en place d'une « *évaluation publique et indépendante* », conduite par « *un comité composé de scientifiques et de spécialistes des questions éthiques dont les rapports seraient rendus publics* ».
Sa démarche n'exclue pas, en outre, l'inscription dans la loi de principes directeurs en forme de « *ligne rouge écartant le risque d'une société de surveillance* » : le principe de subsidiarité, imposant la limitation des usages aux cas « nécessaires » ; le principe d'un contrôle humain « *systématique* » pour prévenir toute délégation : le recours à la reconnaissance faciale doit demeurer « *une aide à la décision* » insiste la mission ; le principe de transparence enfin, compris en l'espèce comme un devoir d'information renforcé « *pour que l'usage des technologies de reconnaissance biométrique ne se fasse pas à l'insu des personnes* ». La mission propose également d'établir quatre interdictions qui réitèrent, en les élargissant, les propositions européennes : interdiction de la notation sociale, à destination des acteurs publics et privés ; interdiction de la catégorisation d'individus en fonction de l'origine ethnique, du sexe, ou de l'orientation sexuelle, sauf dans le cadre de la recherche scientifique et sous réserve de garanties appropriées; interdiction de l'analyse d'émotions, sauf à des fins de santé ou de recherche scientifique et sous réserve de garanties appropriées ; enfin, interdiction de la surveillance biométrique à distance en temps réel dans l'espace public, sauf exception « très limitée » au profit des forces de sécurité. Le rapport précise que cette interdiction porterait, en particulier, sur « *la surveillance biométrique à distance en temps réel lors de manifestations sur la voie publique et aux abords des lieux de culte* ». On peut regretter que cette liste n'implique pas protection des publics vulnérables dans le cadre de rapports d'autorité : en ce sens, le recours à la reconnaissance faciale sur les lieux de travail ou dans en milieu scolaire nous semblent une ligne rouge omise par les sénateurs, qu'impose pourtant un régime de libertés.

Quel régime de garanties et de contrôles ?

L'établissement d'un « régime de redevabilité et de contrôle adapté » est annoncé comme l'une des ambitions majeures portées par la mission. Des distinctions sont opérées pour tenir compte des usages. La première distingue authentification et identification biométriques. L'authentification – jugée, à juste titre, moins intrusive et moins risquée pour les personnes concernées -, ferait l'objet d'un régime plus souple reposant sur quatre volets : en amont, une évaluation de l'impact du système ; en aval, un dispositif permettant de garantir le « *caractère libre, spécifique, éclairé et univoque du consentement donné* » (existence d'une alternative valable, absence de rapport de subordination), l'absence de conservation des images collectées et analysées et le « maintien » d'une supervision humain lors des contrôles d'identité. En matière

d'identification biométrique, une nouvelle distinction est introduite sur la base de la temporalité : l'identification *a posteriori* pourrait être mobilisée dans le cadre d'enquêtes judiciaires ou d'opérations de renseignement, pour la recherche d'auteurs ou de victimes potentielles des infractions les plus graves ou, dans le cadre du renseignement, pour identifier une personne recherchée ou reconstituer son parcours. Le champ des usages potentiels de la reconnaissance faciale à distance en temps réel serait plus restreint. La mission insiste sur le « *caractère particulièrement exceptionnel* » qu'ils devront revêtir. Trois cas « *très spécifiques et circonscrits* » sont envisagés : en matière de police judiciaire, « *pour le suivi d'une personne venant de commettre une infraction grave* » ou la « *recherche dans un périmètre géographique et temporel limité, des auteurs d'infractions graves recherchés par la justice ou des personnes victimes d'une disparition inquiétante* » ; en matière de police administrative, pour la sécurisation de grands évènements présentant « *une sensibilité particulière* » ou les sites *« particulièrement sensibles face à une éventuelle menace terroriste* » ; en matière de renseignement, en cas de « *menaces imminentes pour la sécurité nationale* ». Ces cas d'usage demeurent relativement larges si l'on tient compte de l'interprétation susceptible d'être retenue de la menace terroriste ou la sensibilité d'un site. On saluera toutefois les garanties envisagées pour limiter les atteintes aux libertés : outre la circonscription géographique et temporaire des usages, ceux-ci, nécessairement « *subsidiaires* », seront soumis à un régime d'autorisation préalable des autorités dédiées (magistrat, préfet ou Commission nationale de contrôle des techniques de renseignement en fonction des usages) et un contrôle *a posteriori* dont les contours méritent encore d'être précisés. Les usages devraient en outre, et à cet effet, faire l'objet de mesures de traçabilité, de supervision humaine et d'information adaptée. La mission souhaite interdire toute identification sur la base de données biométriques en temps réel ou en temps différé par des acteurs privés. Enfin, elle n'évince pas la question des moyens en plaidant pour un renforcement de ceux de la CNIL en termes humains, financiers et institutionnels. Il s'agit de permettre à l'autorité, outre d'être systématiquement consultée en amont des déploiements, de procéder à un recensement national de ceux-ci et d'embrasser pleinement un rôle de « *gendarme de la reconnaissance biométrique* ». Ce rapport esquisse ainsi des solutions de compromis intéressantes qui posent, plus largement, ce que pourraient être les premiers jalons d'un régime de redevabilité algorithmique.

Mot clefs

DROIT ET LIBERTE FONDAMENTAUX * Vie privée * Atteinte * Reconnaissance faciale * Protection INFORMATIQUE * Nouvelle technologie * Intelligence artificielle * Reconnaissance faciale.

Peut-être aussi : redevabilité algorithmique.